Department of the Army   OSC Regulation 25-2
Headquarters, US Army
Operations Support Command
1 Rock Island Arsenal
Rock Island, IL 61299-6000   4 April 2002

Information Management

**MANAGEMENT OF OPERATIONS SUPPORT COMMAND (OSC)
PUBLICLY ACCESSIBLE WEBSITES**

_____

<u>Applicability</u>. This regulation applies to all HQ OSC elements
and OSC installations.

<u>Decentralized printing</u>. All OSC installations may locally
reproduce this regulation.

<u>Supplementation</u>. Supplementation of this regulation and
establishment of forms for local use is authorized.

<u>Proponent</u>. The proponent is the Corporate Information Office.
Send comments and suggested improvements to HQ OSC, ATTN:
AMSOS-IMP, 1 Rock Island Arsenal, Rock Island, IL, 61299-6000,
e-mail <u>amsos-ima@osc.army.mil</u>.

<u>Distribution</u>. This publication is distributed electronically
via the OSC Publications Website at
<u>http://www.osc.army.mil/im/rcdsmgt/pubs.htm</u>.

<u>Supersession notice</u>. N/A.

_____
FOR THE COMMANDER:

                         C. R. HOBBY
                         Colonel, GS
                         Chief of Staff

_____
<u>Contents</u>   <u>Paragraph</u>

1. <u>Purpose</u>. This regulation delineates the policy, provides guidance, and assigns responsibility related to establishing, operating, and maintaining OSC publicly accessible websites.

2. <u>References</u>.

    a. AR 25-1, Army Information Management Program.

    b. AR 25-55, Army Freedom of Information Act Program.

    c. AR 360-1, The Public Affairs Program.

    d. AR 380-5, Department of the Army Information Security Program.

    e. AR 380-19, Information Systems Security.

    f. DoD Directive 8910.1 Management and Control of Information Requirements.

    g. DOD Web Site Administration Policies & Procedures, 25 Nov 98.

    h. OSCR 360-1, Public Affairs.

    i. OSC CG Policy Memo 44, Use of OSC Communications Systems and Other Resources.

    j. Public Law 100-235, Computer Security Act of 1987.

3. <u>Definitions</u>.

    a. <u>Publicly accessible web site</u>. A web site that contains releasable information and is accessible to the general public over the Internet. For the purposes of this regulation, the terms "publicly accessible web site" and "Internet web site" are synonymous.

    b. <u>Web master</u>. The individual responsible for a web server. This person is the single point of contact for all issues associated with the web server.

    c. <u>Page master</u>. This person is responsible for a web page. This responsibility includes all facets of a web page including, but not limited to, the functionality of a web page as well as the data contained on that page.

4. <u>Policies</u>.

    a. It is fully appropriate for OSC organizations to establish and maintain publicly accessible websites, provided they support legitimate, mission-related activities of the Army, and are consistent with prudent operational and security considerations.

    b. Consistent with other leadership responsibilities for public communication, the decision whether or not to establish an organizational web site, and to publish appropriate instructions and regulations for a web site within the limitations established by this document, is hereby delegated to each OSC organization. For the purposes of this document, an OSC organization is an HQ OSC directorate, business center, special staff office, project team, the Field Support Command, and other OSC subordinate installations.

    c. Web page content must be suitable for audiences that may include non-military viewers. Ensure that information residing on a server with an "army.mil" domain cannot be interpreted as reflecting official Department of the Army (DA) policies or positions. Ensure that the information posted is consistent with official policies and positions.

    d. Each organization operating a publicly accessible web site will implement technical security best practices with regard to its establishment, maintenance, and administration.

    e. All OSC publicly accessible websites will be DA accredited and registered with appropriate agencies. All DA organizations are required to register their publicly accessible websites, web publications, FOIA electronic reading room documents, and library sources IAW the Government Information Locator Service (GILS). The Corporate Information Directorate (AMSOS-IM) and the Public Affairs Office (AMSOS-PA) will register the OSC Home Page with GILS. HQ organization sites within the "osc.army.mil" domain are included in the registration of the OSC Home Page. Installations must register their sites separately.

    f. Ensure that all information is current, accurate, factual, related to the mission of the command organization, and professionally presented. Ensure the page does not contain duplicate information existing elsewhere within OSC publicly accessible sites or information that is the responsibility of another organization or installation.

g.   HQ OSC chiefs and OSC installation commanders must ensure that information provided on any of their information sites does not contain classified or Privacy Act information, or information that could enable the recipient to infer classified or unclassified sensitive information, either from individual segments of the information, or from the aggregate of informa-tion available. It is the commander's discretion to authorize, deny, or terminate organization websites based on the web site's ability to provide a value-added service, its enhancement of the organization's mission, or to realize efficiencies.

h.   Publicly accessible web sites CANNOT contain items identifying employees' spouses, their children, or other personal information. Do not use personnel photos or post individual office telephone numbers. A statement such as "individuals in this office can be reached at (give a single office phone number)" may be used.

i.   All OSC publicly accessible web sites must identify the page master responsible for the site, an e-mail address, and the date when the pages were last modified or reviewed.

j.   Obtain the owner's permission when reproducing, distributing, or publicly performing copyrighted materials.

k.   All web pages are subject to US Army Operations Security (OPSEC) reviews.

l.   All web pages must be reviewed by the HQ OSC Public Affairs Office before posting, and periodically thereafter.

m.   The design of all web pages will conform to the Federal Information Technology Accessibility Standards (Section 508).

n.   The design of web pages will conform to the OSC Page Design Standards.

o.   Links to other websites.

(1)   Links to civilian or military organizations, and programs and projects related to the mission and function of the organization, are authorized.

(a)   Do not create software download links to non-DoD sources and commercially (licensed) software.

(b) Do not create links to pages that support political views. They give the appearance that the OSC is endorsing a particular political faction or viewpoint.

(c) The military, inlcuding OSC organizations, cannot endorse a product, or organization, or exercise any responsibility over the contents at the destination pointed to by a link.

(d) Display the following disclaimer when linking to non-DoD sites. This disclaimer may appear on the page(s) listing external links or through an intermediate "exit notice" page generated by the server whenever a request is made for any site outside of the official information service (usually the .mil domain).

"*The appearance of these hyperlinks does not constitute endorsement by the Operations Support Command (OSC) of these websites or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the OSC does not exercise any editorial control over the information you may find at these locations. These links are provided consistent with the stated purposes of this military web site.*"

(e) Commanders must realize that once the decision is made to include a link to one non-military site, the command may have to link to all similar sites.

(f) Graphics or logos depicting commercial companies or products will not appear on OSC publicly accessible web sites.

(2) Review all external links periodically to ensure their continued suitability and availability. Remove all questionable or objectionable links.

p. Official Army web information services cannot offer commercial sponsorships, advertisements, and endorsements. Commanders will ensure that association with commercial sponsorships, advertisements or endorsements does not adversely affect the credibility of official information.

q. Forms, Information Collection, and Usage Statistics.

(1) As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness

of web information services. Collection of data such as the most or least requested documents, type of browser software used to access the web information service, etc., is appropriate. Collected data must be destroyed in 2 years, unless otherwise directed.

        (2)   DoD Web Site Administration Policies & Procedures, 25 Nov 98, prohibited methods of collecting user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors from the public. "Cookies" may be used with other methods to collect non-user identifying information to customize user sessions; however, notify users in advance of what and why information will be collected and how it will be used.

    r.   Web browser software.

        (1)   The standard browser is Internet Explorer (preferred) or Netscape. An installation may choose which of the above browsers to support. Establish procedures concerning the use of various plug-ins so that a malicious code will not compromise the system.

        (2)   Use and distribution of any software must comply with the applicable software licensing restrictions and agreements on Internet Index Server (IIS).

    s.   Public web servers will be exclusive, i.e., the machine operating as such will not be used to store anything other than publicly releasable information, even in areas or directories which are not shared to the internet.

5.   Responsibilities.

    a.   The OSC Public Affairs Officer (AMSOS-PA) will:

        (1)   Establish a process for the identification of information appropriate for posting to publicly accessible web-sites and ensure it is consistently applied.

        (2)   Ensure the review of information for security, levels of sensitivity, and other concerns before release.

        (3)   Ensure the accuracy, consistency, appropriateness, and timeliness of all information placed on the web site.

(4)   Conduct annual review of all HQ OSC and subordinate sites for compliance with established Public Affairs (PA) guidance for appropriateness of information. PA will notify page masters of any non-compliant Information.

(5)   Ensure the establishment of procedures for management oversight and regular functional reviews of the web site.

b.   The Director, Corporate Information (AMSOS-IM), will:

(1)   Provide policy and procedural guidance with respect to establishing, operating, and maintaining OSC websites.

(2)   Approve and publish instructions and publications, as necessary, to guide, direct, or help OSC publicly accessible web site activities.

(3)   Establish architectural and infrastructure guidelines for OSC web servers and user access to the hardware and software.

c.   Information Assurance Manager (IAM) (AMSOS-IMP) will:

(1)   Ensure Internet users are aware of the Internet's vulnerabilities; their individual responsibilities; limitations of access; and the approval process for release of US Government information.

(2)   Ensure the use of approved DoD security and privacy notices and applicable disclaimers on all web sites under their purview.

(3)   Ensure that a comprehensive, multi-disciplinary security assessment is conducted of their websites within 120 days of the promulgation of this document and at least annually thereafter.

(4)   Ensure compliance with this policy for those functions, missions, agencies, and activities in their purview.

(5)   Maintain the operational integrity and security of the computer and the network supporting the web site.

d.   The Force Protection and Intelligence Directorate (AMSOS-FP) will ensure all information placed on publicly accessible websites is appropriate for worldwide dissemination

and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

    e.   Web master will:

        (1)   Monitor professional appearance of web pages.

        (2)   Establish procedures for updates to web site content.

    f.   Web server systems administrator will:

        (1)   Install and maintain web server hardware and software.

        (2)   Maintain web server security.

        (3)   Administer user rights.

        (4)   Perform anti-virus functions and procedures.

        (5)   Ensure the maintenance of server hardware and software platforms.

        (6)   Ensure the administration of user access.

        (7)   Ensure information assurance hardware and software are maintained.

        (8)   Ensure the proper installation, configuration, and maintenance of Internet access software.

        (9)   Ensure the maintenance of OSC Internet access logs.

        (10)   Ensure mechanisms are in place to control access to the OSC publicly accessible web sites as appropriate.

        (11)   Ensure compliance with this policy.

        (12)   Remove non-compliant sites.

   g.   HQ OSC chiefs and OSC installation commanders, or their designated representative, will:

       (1)   Establish procedures to ensure that classified, Privacy Act information, or information that could enable the recipient to infer classified or unclassified sensitive information, from individual segments of the information, or from the aggregate of the information, is not posted to OSC publicly accessible web sites and that classified information is not transmitted to the Internet.

       (2)   Establish procedures for the periodic review of newsgroups, bulletin boards, and web pages maintained by their offices to ensure the postings do not adversely affect the OSC.

    h.   Page masters and content providers will take responsibility for periodically reviewing and making sure their web pages conform to this guidance. Reviews will be completed semiannually.